

~~SECRET~~

DC 10 1/11

File

INTELLIGENCE COMMUNITY SECURITY PROBLEMS:

A SUMMARY REPORT

24 September 1973

A. PURPOSE

1. To stimulate intelligence community action on security policies and procedures to achieve optimum use of intelligence products without forfeiting adequate security protection of intelligence and intelligence sources and methods.

B. INTRODUCTION

2. Policies and procedures for supervising the dissemination and security of intelligence materials and protecting intelligence sources and methods have been developed at different times and under different authorities since World War II. Presently they are administered by fragmented and dispersed authorities, lack consistency in application, may arbitrarily limit the flow of sensitive information to community producers with a need to know, and may be internally inconsistent with other guiding directives and regulations on the books.

2. These problems are most apparent in the various compartmentation systems and in procedures for controlling release of intelligence to foreign governments. The middle and senior level man years spent in accommodating to or administering the various security systems in the community are incalculable at this time but certainly represent an inefficient use of resources and an inhibiting factor in improving the quality, scope and timeliness of the community's product.

3. While the USIB Security Committee would appear to be a logical focus for handling of problems relating to compartmented intelligence and release of intelligence to foreign governments, such is not within its presently assigned mission and the committee is not staffed to deal with such responsibilities. The Security Committee chairman also has a full-time assignment as Director of Security, CIA. The committee has only two full-time personnel, one professional and one clerical.

4. The USIB Committee Survey Task Group Report, August 1973, noted that aside from its activities in the investigations of "leaks" of intelligence to public media, the Security Committee appears to be a rather inactive organ. Its one subordinate element, the Computer Security Sub-Committee, is involved with a community issue which appears to be more closely related to the USIB Intelligence Information Handling Committee (IHC) concerns and communications issues than to the Security Committee problem area.

25X1

~~SECRET~~

SECRET**C. COMPARTMENTATION**

5. The intelligence community's vastly increased technological capabilities have resulted in a commensurate increase in the volume of compartmented intelligence and intelligence information. The present compartmentation systems, however, were designed to handle smaller and simpler situations. As they have grown to accommodate new collection systems and an increasing volume of products, they are reaching the point of near impracticality and may prove even more limiting as the community moves into near-real-time readout, reporting systems.

6. Two factors deserving of attention are those of costs and mutual reinforcement.

a. There are costly differences in many functional areas of concern; e.g., determination of personnel access, physical security standards, document and communications controls, dissemination limitations, and sanitization and decontrol measures.

b. Compartmentation and classification systems are not always mutually reinforcing. Materials which are compartmented in a system intended to deal only with substantive information can and sometimes do reveal operational capabilities which are intended to be protected by a separate operational compartmentation.

25X1

8. Present directives, regulations and manuals do not set forth a clear and comprehensive statement of policy concerning the objectives and criteria for the compartmentation of sensitive intelligence and intelligence information in proper balance with consumer and management needs.

9. The need to maintain on-going operational compatibility with general practice under existing community-wide compartmentation systems limits the scope of changes in practice which any single department or agency can effect unilaterally in its own behalf. Community action will be needed to improve the situation.

10. Compartmentation systems need to be brought up-to-date to meet the new demands the intelligence community will be facing for the timely processing, reporting and use of sensitive information

SECRET

SECRET

which will result from the new and continuing high-volume collection sources in the foreseeable future.

11. Suggested actions include:

a. A review of sensitive intelligence sources and methods, and information from them or derived from them, which warrant protection from unauthorized disclosure additional to that provided by classification controls under E.O. 11652 and dissemination controls under DCID 1/7.

b. Formulation of "need to know" criteria for personnel access to such materials.

c. Centralization of responsibility and authority to develop and administer controls and procedures for protecting compartmented intelligence and intelligence information.

d. Updating of guidance documents establishing and controlling the compartmentation of intelligence and intelligence information.

e. Simplification of dissemination procedures for compartmented information, including packaging and distribution methods and possible consolidation of separate registeries.

f. Formulation and approval of a single system for compartmenting intelligence and intelligence information, by category, as appropriate.

D. RELEASE OF INTELLIGENCE TO FOREIGN GOVERNMENTS

12. A recent IC staff study, subject as above, of 25 May 1973, prepared in response to a Management Committee action, has shown that:

a. The present arrangement for accomplishing releases of intelligence to foreign governments are complex and to a considerable degree decentralized.

b. No system currently exists to provide a complete picture of the U.S. intelligence that is being released.

c. The degree to which disclosures are kept in synchronism with U.S. policy depends on the sensitivity with which intelligence organizations and even individual releasing officers are able to discern unannounced changes in policy.

SECRET

SECRET

13. The study further pointed out that there is a lack of consistency among the existing release arrangements and agreements, and little coordination among multiple relationships within individual foreign countries. Within the intelligence community there are considerable differences in practices relating to the release of departmental intelligence.

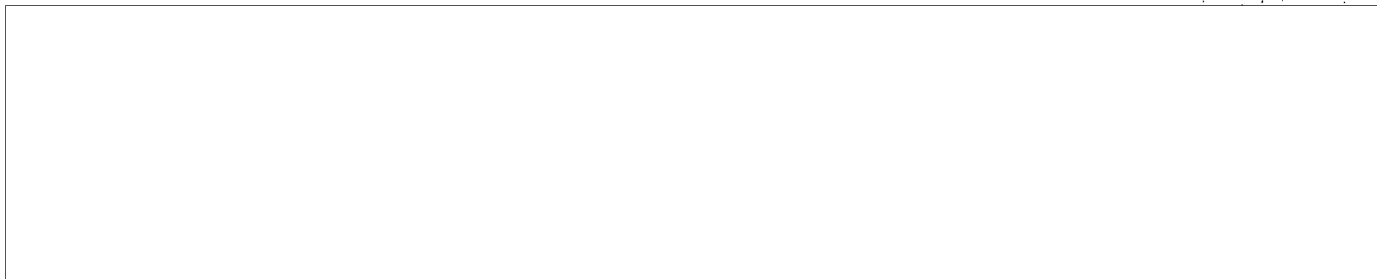
14. Several steps could be taken to enable the DCI to bring more order and coherence into the disclosure of intelligence to foreign governments and international organizations and to enhance the linkage of such releases with U.S. policy interests and security arrangements. Initially there is a need to assemble, collate and analyze relevant information. There should be a review of all Second and Third Party substantive intelligence exchange agreements to assure the DCI that: (a) all agreements reflect current U.S. policy toward the country or international organization involved; (b) continuing agreements provide for a release of intelligence at the minimum level consistent with U.S. net advantage; and (c) all agreements with a particular country reflect a consistent policy and guidance.

15. Linked to but independent of this review would be the establishment of an interagency mechanism to keep intelligence release authorities cognizant of applicable U.S. policy objectives. At a minimum, this mechanism should involve the NSC, State Department, Department of Defense and CIA. The purpose of establishing such a mechanism would be to afford guidance to personnel responsible for the release of intelligence to foreign governments, and to reduce the "guesswork" element in the field and the risk that intelligence disclosures could run counter to particular U.S. objectives.

16. Concurrently, a system should be established to keep the DCI advised as to what intelligence is being released to what governments and for what purposes. Review and analysis of the information assembled through these measures would enable the DCI to alert USIB member agencies to particular concerns about the release problem and to define DCI criteria governing disclosure.

E. TECHNICAL SURVEILLANCE COUNTERMEASURES

25X1



4
SECRET

SECRET

25X1

18. The primary function of the TSCC, as described in The USIB Committee Survey Task Group Report of August 1973 has been to promote and coordinate the development and use of the means to defend U.S. personnel and facilities against penetration by technical surveillance. The Survey Task Group reported the real value of the committee appears to have stemmed from the knowledgeability and energy of the TSCC chairman in seeking out and finding problem areas upon which he could bring to bear the force of a coordinated community position or a reasonable arbitration. This chairman retired in June 1973 as also did the only other full-time member of the TSCC professional staff.

19. The Survey Task Group found that normal TSCC concerns tended to overlap considerably with the activities of the Security Committee and concluded that the TSCC functions could best be handled in a reorganized effort of the Security Committee. One reason for this conclusion was that the TSCC effort had involved activities in problem areas which often transcended the explicit concerns of the TSCC mission -- thanks to the efforts of and effectiveness of the then-TSCC chairman -- but the Group considered it doubtful that any succeeding chairman could operate in this manner.

F. CONCLUSIONS

20. Restrictive and outmoded intelligence community security policies and procedures are an impediment to DCI efforts to improve the quality, scope and timeliness of the community's product and to achieve a more efficient use of resources involved in the handling of compartmented information.

21. Presently there is no centralized body in the intelligence community with the authority to address community-wide security problems of broad scope, to conduct the studies required, and to formulate and monitor the implementation of new security procedures adequate to manage and use the high volume of new intelligence information anticipated in the foreseeable future.

22. Meeting the need for competent professional support and community involvement to carry out these tasks can be facilitated through the establishment of a reconstituted USIB Security Committee with a full-time chairman and requisite full-time staff, and broader functions than are assigned to the present committee.

SECRET

SECRET

23. The mission and activities of the TSCC could logically be assigned to the reconstituted Security Committee.

G. RECOMMENDATIONS

24. It is recommended that:

a. The USIB Security Committee be reconstituted and reorganized with a full-time Chairman and appropriate full-time staff.

b. The new Security Committee be tasked to formulate and recommend to the DCI new policies and procedures to resolve the problems cited in this report and such other security problems as may be brought to its attention by the USIB or the DCI, and be delegated authority requisite to the fulfillment of its responsibilities.

c. DCID 1/11, "Security Committee," effective 23 April 1965, and DCID 1/12, "Technical Surveillance Counter-measures Committee," 23 December 1964, be rescinded and replaced by a new DCID which defines the mission and functions of a new USIB Security Committee having responsibilities in the fields of intelligence compartmentation, release of intelligence to foreign governments, and technical surveillance counter-measures, in addition to the responsibilities of the present Security Committee.

SECRET

SECRET**INTELLIGENCE COMMUNITY SECURITY PROBLEMS:****A SUMMARY REPORT****24 September 1973****A. PURPOSE**

1. To stimulate intelligence community action on security policies and procedures to achieve optimum use of intelligence products without forfeiting adequate security protection of intelligence and intelligence sources and methods.

B. INTRODUCTION

2. Policies and procedures for supervising the dissemination and security of intelligence materials and protecting intelligence sources and methods have been developed at different times and under different authorities since World War II. Presently they are administered by fragmented and dispersed authorities, lack consistency in application, may arbitrarily limit the flow of sensitive information to community producers with a need to know, and may be internally inconsistent with other guiding directives and regulations on the books.

2. These problems are most apparent in the various compartmentation systems and in procedures for controlling release of intelligence to foreign governments. The middle and senior level man years spent in accommodating to or administering the various security systems in the community are incalculable at this time but certainly represent an inefficient use of resources and an inhibiting factor in improving the quality, scope and timeliness of the community's product.

3. While the USIB Security Committee would appear to be a logical focus for handling of problems relating to compartmented intelligence and release of intelligence to foreign governments, such is not within its presently assigned mission and the committee is not staffed to deal with such responsibilities. The Security Committee chairman also has a full-time assignment as Director of Security, CIA. The committee has only two full-time personnel, one professional and one clerical.

4. The USIB Committee Survey Task Group Report, August 1973, noted that aside from its activities in the investigations of "leaks" of intelligence to public media, the Security Committee appears to be a rather inactive organ. Its one subordinate element, the Computer Security Sub-Committee, is involved with a community issue which appears to be more closely related to the USIB Intelligence Information Handling Committee (IHC) concerns and communications issues than to the Security Committee problem area.

25X1
25X1**SECRET**

SECRET

C. COMPARTMENTATION

5. The intelligence community's vastly increased technological capabilities have resulted in a commensurate increase in the volume of compartmented intelligence and intelligence information. The present compartmentation systems, however, were designed to handle smaller and simpler situations. As they have grown to accommodate new collection systems and an increasing volume of products, they are reaching the point of near impracticality and may prove even more limiting as the community moves into near-real-time readout reporting systems.

6. Two factors deserving of attention are those of costs and mutual reinforcement.

a. There are costly differences in many functional areas of concern; e.g., determination of personnel access, physical security standards, document and communications controls, dissemination limitations, and sanitization and decontrol measures.

b. Compartmentation and classification systems are not always mutually reinforcing. Materials which are compartmented in a system intended to deal only with substantive information can and sometimes do reveal operational capabilities which are intended to be protected by a separate operational compartmentation.

25X1

8. Present directives, regulations and manuals do not set forth a clear and comprehensive statement of policy concerning the objectives and criteria for the compartmentation of sensitive intelligence and intelligence information in proper balance with consumer and management needs.

9. The need to maintain on-going operational compatibility with general practice under existing community-wide compartmentation systems limits the scope of changes in practice which any single department or agency can effect unilaterally in its own behalf. Community action will be needed to improve the situation.

10. Compartmentation systems need to be brought up-to-date to meet the new demands the intelligence community will be facing for the timely processing, reporting and use of sensitive information

SECRET

~~SECRET~~

which will result from the new and continuing high-volume collection sources in the foreseeable future.

11. Suggested actions include:

a. A review of sensitive intelligence sources and methods, and information from them or derived from them, which warrant protection from unauthorized disclosure additional to that provided by classification controls under E.O. 11652 and dissemination controls under DCID 1/7.

b. Formulation of "need to know" criteria for personnel access to such materials.

c. Centralization of responsibility and authority to develop and administer controls and procedures for protecting compartmented intelligence and intelligence information.

d. Updating of guidance documents establishing and controlling the compartmentation of intelligence and intelligence information.

e. Simplification of dissemination procedures for compartmented information, including packaging and distribution methods and possible consolidation of separate registeries.

f. Formulation and approval of a single system for compartmenting intelligence and intelligence information, by category, as appropriate.

D. RELEASE OF INTELLIGENCE TO FOREIGN GOVERNMENTS

12. A recent IC staff study, subject as above, of 25 May 1973, prepared in response to a Management Committee action, has shown that:

a. The present arrangement for accomplishing releases of intelligence to foreign governments are complex and to a considerable degree decentralized.

b. No system currently exists to provide a complete picture of the U.S. intelligence that is being released.

c. The degree to which disclosures are kept in synchronism with U.S. policy depends on the sensitivity with which intelligence organizations and even individual releasing officers are able to discern unannounced changes in policy.

~~SECRET~~

SECRET

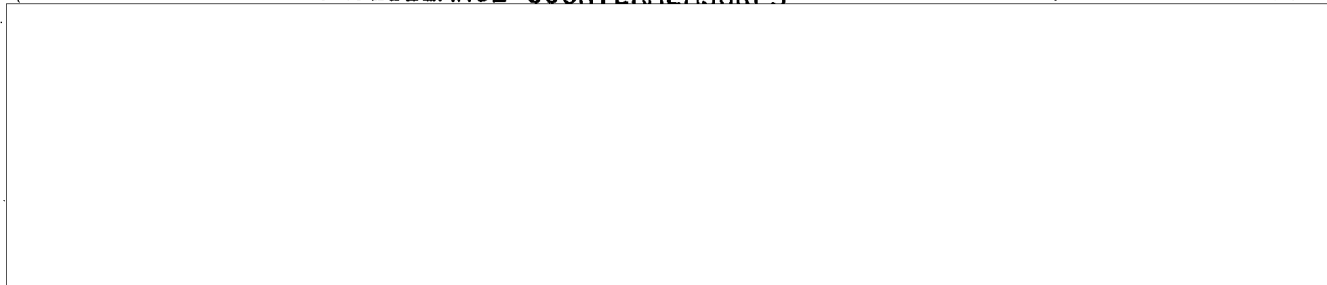
13. The study further pointed out that there is a lack of consistency among the existing release arrangements and agreements, and little coordination among multiple relationships within individual foreign countries. Within the intelligence community there are considerable differences in practices relating to the release of departmental intelligence.

14. Several steps could be taken to enable the DCI to bring more order and coherence into the disclosure of intelligence to foreign governments and international organizations and to enhance the linkage of such releases with U.S. policy interests and security arrangements. Initially there is a need to assemble, collate and analyze relevant information. There should be a review of all Second and Third Party substantive intelligence exchange agreements to assure the DCI that: (a) all agreements reflect current U.S. policy toward the country or international organization involved; (b) continuing agreements provide for a release of intelligence at the minimum level consistent with U.S. net advantage; and (c) all agreements with a particular country reflect a consistent policy and guidance.

15. Linked to but independent of this review would be the establishment of an interagency mechanism to keep intelligence release authorities cognizant of applicable U.S. policy objectives. At a minimum, this mechanism should involve the NSC, State Department, Department of Defense and CIA. The purpose of establishing such a mechanism would be to afford guidance to personnel responsible for the release of intelligence to foreign governments, and to reduce the "guesswork" element in the field and the risk that intelligence disclosures could run counter to particular U.S. objectives.

16. Concurrently, a system should be established to keep the DCI advised as to what intelligence is being released to what governments and for what purposes. Review and analysis of the information assembled through these measures would enable the DCI to alert USIB member agencies to particular concerns about the release problem and to define DCI criteria governing disclosure.

E. TECHNICAL SURVEILLANCE COUNTERMEASURES

**SECRET**

SECRET

25X1

18. The primary function of the TSCC, as described in The USIB Committee Survey Task Group Report of August 1973 has been to promote and coordinate the development and use of the means to defend U.S. personnel and facilities against penetration by technical surveillance. The Survey Task Group reported the real value of the committee appears to have stemmed from the knowledgeability and energy of the TSCC chairman in seeking out and finding problem areas upon which he could bring to bear the force of a coordinated community position or a reasonable arbitration. This chairman retired in June 1973 as also did the only other full-time member of the TSCC professional staff.

19. The Survey Task Group found that normal TSCC concerns tended to overlap considerably with the activities of the Security Committee and concluded that the TSCC functions could best be handled in a reorganized effort of the Security Committee. One reason for this conclusion was that the TSCC effort had involved activities in problem areas which often transcended the explicit concerns of the TSCC mission -- thanks to the efforts of and effectiveness of the then-TSCC chairman -- but the Group considered it doubtful that any succeeding chairman could operate in this manner.

F. CONCLUSIONS

20. Restrictive and outmoded intelligence community security policies and procedures are an impediment to DCI efforts to improve the quality, scope and timeliness of the community's product and to achieve a more efficient use of resources involved in the handling of compartmented information.

21. Presently there is no centralized body in the intelligence community with the authority to address community-wide security problems of broad scope, to conduct the studies required, and to formulate and monitor the implementation of new security procedures adequate to manage and use the high volume of new intelligence information anticipated in the foreseeable future.

22. Meeting the need for competent professional support and community involvement to carry out these tasks can be facilitated through the establishment of a reconstituted USIB Security Committee with a full-time chairman and requisite full-time staff, and broader functions than are assigned to the present committee.

SECRET

SECRET

23. The mission and activities of the TSCC could logically be assigned to the reconstituted Security Committee.

G. - RECOMMENDATIONS

24. It is recommended that:

a. The USIB Security Committee be reconstituted and reorganized with a full-time Chairman and appropriate full-time staff.

b. The new Security Committee be tasked to formulate and recommend to the DCI new policies and procedures to resolve the problems cited in this report and such other security problems as may be brought to its attention by the USIB or the DCI, and be delegated authority requisite to the fulfillment of its responsibilities.

c. DCID 1/11, "Security Committee," effective 23 April 1965, and DCID 1/12, "Technical Surveillance Counter-measures Committee," 23 December 1964, be rescinded and replaced by a new DCID which defines the mission and functions of a new USIB Security Committee having responsibilities in the fields of intelligence compartmentation, release of intelligence to foreign governments, and technical surveillance counter-measures, in addition to the responsibilities of the present Security Committee.

SECRET

SECRET

5 NOV 1973

MEMORANDUM FOR: CIA Member, U. S. Intelligence Board

ATTENTION : Mr. Don M. Huebner, Special Assistant
for NSC and USIB Affairs, O/DDI

SUBJECT : Proposed New DCID 1/11, "Security Committee"

1. Reference is made to your request of 26 October 1973 for comments on proposed new DCID 1/11.

2. Paragraphs 2.e., page 2, and 3.a.(7), page 4, should be amended to include classified military intelligence which is released under the control of the National Disclosure of Military Information Policy Committee (NDPC). We recommend this change because we believe that the DCI's responsibility to protect intelligence sources and methods would be enhanced if the Security Committee became involved in the release of classified military intelligence to foreign governments and international organizations.

3. In addition, we recommend that the proposed new DCID contain statements of mission and functions covering computer security, an activity of significant importance. As you are aware, the current Security Committee has established an active Computer Security Subcommittee.

4. In our review we have noted that the proposed new DCID lists statements of mission in functional terms. It also has statements of functions. We further noted on page 1 of the proposed new DCID a reference to NSCID No. 5. Unless the author is referring to a new NSCID No. 5 not yet released, we can see no relationship between the two.

5. There is a reference in paragraph 3.a.(4), page 3, to "scientific evaluation methodology." We assume this refers to polygraph. If it does, we do not believe it should be a

25X1

SECRET

SECRET


function of the Security Committee. We would prefer to leave the formulation of CIA polygraph policies and procedures in the CIA Office of Security.

6. The draft DCID appears to be longer and in greater detail than most other DCID's.

7. Attached is an amended draft covering items mentioned above.

8. Please advise if any additional data are desired.

25X1



CIA Member, Security Committee

Att:

SECRET

SECRET

USIB-D-5.1/21

24 October 1973

UNITED STATES INTELLIGENCE BOARD

MEMORANDUM FOR THE UNITED STATES INTELLIGENCE BOARD

SUBJECT : Proposed New DCID 1/11, "Security Committee"

1. The Director of Central Intelligence has authorized circulation of the enclosed proposed DCID 1/11, "Security Committee" for consideration by the USIB.

2. The draft DCID would establish a new "Security Committee" with expanded functions and a full-time chairman and staff. The functions of the new committee would include those formerly assigned to the Security Committee and to the Technical Surveillance Countermeasures Committee (TSCC). On the effective date of the establishment of the "Security Committee," DCID 1/11, 23 April 1965 and DCID 1/12, 23 December 1964, will be cancelled.

3. It is planned to schedule this item on a USIB agenda for discussion at an early meeting.

25X1



Acting Executive Secretary

Enclosure

25X1

SECRET



CLASSIFIED
TOP SECRET
NSCIR D-5 1/21
OCTOBER 1973F
TDIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11^{1/}Security Committee

(Effective _____)

The United States Intelligence Board's Security Committee as established by DCID 1/11, 23 April 1965, and the United States Intelligence Board's Technical Surveillance Countermeasures Committee as established by DCID 1/12, 23 December 1964, are hereby terminated. Pursuant to provisions of Subsection 102 (d) of the National Security Act of 1947, as amended, to provisions of NSCID No. 1 and NSCID No. 5, and to paragraph 2.b. of NSAM No. 317 with respect to technical surveillance countermeasures, a new standing committee of USIB is hereby established.

1. Name of the Committee

The committee will be known as the Security Committee.

2. Mission

The mission of the committee, under the general guidance of the Director of Central Intelligence is to:

Promote means by which

a. Advise and assist the DCI ^{can} in the discharge of his duties and responsibilities under NSCID No. 1, with respect to the protection of ^{U.S. foreign} intelligence and intelligence sources and methods from

^{1/} Supersedes DCID 1/11, effective 23 April 1965, and DCID 1/12, effective 23 December 1964

Unauthorized disclosure, ^{2/} NSCID No. 5, with respect to counter-intelligence matters abroad; and paragraph 2.b. of NSAM 317, with respect to technical surveillance countermeasures conducted by the intelligence community.

b. ^{Promote} Develop, ~~coordinate, promote and monitor utilization of~~ practical security standards and ^{procedures} ~~practices~~, including effective defense of US personnel and installations against penetration by technical surveillance equipment and techniques;

c. ^{Promote} Review ~~compartmentation procedures~~ ^{3/} and foster the objectives of achieving optimum use of ^{compartmented} intelligence products and improving the effectiveness and coordination of ^{compartmented} intelligence activities consonant with realistic security procedures for the protection of sources and methods;

Promote means to ^{to}
d. /Limit damage to ~~intelligence and~~ intelligence sources and methods in instances of unauthorized disclosure; and

Promote means by which appropriate consideration is given
e. ~~Review procedures and develop standards for the release~~ to all release of U. S. foreign intelligence to foreign governments, ~~in of US intelligence to foreign governments.~~ cluding that military intelligence released under the auspices of the

National Disclosure of Military Information Policy Committee (NDPC).

f. Promote practical computer security ^{Policy,} standards, and procedures for the protection of U. S. foreign intelligence information.

2/ Unauthorized disclosure includes but is not limited to loss, compromise or any revelation of classified information to unauthorized persons and embraces disclosure by technical penetration.

3/ The systematic compartmentation of certain categories of finished intelligence, raw intelligence information, and intelligence sources and methods is required by special and separate directive controls.

3. Functions

The functions of the committee are:

a. General

(1) To recommend^{4/} to the DCI and to coordinate and monitor implementation of policies, directives, guidance and procedures for the protection of finished intelligence,^{U. S. foreign} intelligence information, and intelligence sources and methods from unauthorized disclosure, including technical surveillance countermeasures ~~and to recommend to the DCI such modifications as circumstances may from time to time require.~~

(2) To formulate and recommend^{to the DCI}/compatible and standard markings for intelligence documents and materials under classification, compartmentation and dissemination controls.

(3) To advise and assist the DCI, as appropriate, with respect to coordinated implementation of intelligence community policies and procedures regarding^{downgrading and classified} intelligence and intelligence information/^{and materials} pursuant to statute, executive order, or other authority and in consonance with the DCI's statutory responsibility for the protection of intelligence sources and methods.

(4) To formulate, recommend^{to the DCI}/and monitor intelligence community policies and procedures for personnel security clearance, indoctrination and re-indoctrination, including, but not limited to: security-related obligations and conditions of employment; personnel security approval criteria; investigative requirements, ~~including scientific evaluation methodology as appropriate~~; and compatible and complementary security education, supervisory and review programs.

^{4/} Recommendations shall be consonant with the responsibility of each department and agency for the protection of intelligence and of intelligence sources and methods within its own organization from unauthorized disclosure.

(5) To review ^{personnel and physical} security standards and practices ^{all} applicable to Government departments and agencies and their contractors as such standards and practices relate to the protection of intelligence and of intelligence sources and methods, and to formulate ^{to the DCI} and recommend/appropriate technical criteria and standards in consideration of the effectiveness, risk and cost factors involved, to include recommendations as to proposals for legislation.

(6) ^{To recommend to the DCI} ~~To standardize, simplify and integrate~~ policies and ^{standardized and simplified} procedures for the establishment and maintenance of ~~appropriate~~ compartmentation systems, dissemination systems, and sanitization, declassification and decontrol systems.

(7) To review procedures and directives governing the release to foreign governments and international organizations ^{U. S. foreign} including classified military intelligence of intelligence, ~~for which the DCI has release authority~~, and to develop guidance and recommendations for improving the standards ^{U. S. foreign} under which such release of both substantive intelligence and intelligence related equipment is made, with particular attention to insuring that the release of ^{foreign} US/intelligence is consonant with US policy toward the governments involved, and results in net advantage to the United States, and the information itself is afforded a degree of protection equivalent to that

(8) To advise and assist other USIB committees, and ^{afforded by the United States.} such national intelligence offices as request it, on the technical aspects of methods and procedures for the authorized dissemination, release or disclosure of US finished intelligence, intelligence information, and intelligence sources and methods to the public, foreign governments or international organizations in which the US Government participates.

^{for}
(9) To develop and ~~recommend~~ to the DCI policies and procedures to ~~insure adequate protection of U. S. foreign~~ intelligence data stored and processed by computer.

~~other~~ (10) To advise and assist the DCI, USIB Committees, and ~~such national intelligence offices as request it,~~ ^{~~element Components~~} with respect to ^{all} ~~intelligence community~~ computer security issues.

(11) To act as a forum for coordinated intelligence community efforts to resolve security problems in the computer environment.

(12)
(9) To call upon departments and agencies, as appropriate, to investigate within their department or agency any unauthorized disclosure of ^{U.S. foreign} intelligence, intelligence information, or intelligence sources and methods; and to report these investigations to the DCI, through USIB, together with (a) an assessment of the impact on the US intelligence process and any foreseeable implications to national security or relations with foreign countries as a result of use of the information gained through the unauthorized disclosure, (b) corrective measures taken or needed within departments and agencies involved in order to prevent such disclosures in the future or to minimize the adverse effects of the case at hand, and (c) recommendations concerning any appropriate additional actions.

b. With respect to general technical surveillance countermeasures:

(1) To facilitate the formulation, development and application of effective countermeasures equipment and techniques based on assessments by the Central Intelligence Agency and other knowledgeable member agencies of USIB of (a) the state of the art of audio surveillance equipment, and (b) the known and estimated technical surveillance capabilities of foreign governments.

(2) To formulate and recommend to the DCI resource programming objectives for USIB departments and agencies in the field of technical surveillance countermeasures in consideration of current and foreseen threats and with regard for the effective and efficient use of resources.

(3) To coordinate all aspects of the US Government effort in defense against technical surveillance penetration and to resolve conflicts that may arise in connection therewith.

(4) To facilitate the interchange of information in the field of technical surveillance countermeasures among USIB departments and agencies and others as appropriate, particularly by the preparation, publication and dissemination of appropriate reports, notices and guides.

(5) To recommend policies governing disclosures concerning technical surveillance devices (except as otherwise provided for under NSCID No. 5), or countermeasures thereto, to be made to foreign governments or international organizations in which the US Government participates.

(6) To advise USIB departments and agencies of technical surveillance countermeasures objectives and standards to be considered in connection with existing or new facilities abroad.

(7) To prepare damage assessments by furnishing reports of known or suspected hostile audio surveillance penetrations of US facilities and recommending remedial or other actions as appropriate.

(8) To evaluate the curriculum and operations of,
and to provide policy guidance [redacted]
[redacted] common concern
for the training in technical surveillance countermeasures of USIB
and other US Government department and agency personnel.

(9) To evaluate technically the foreign technical surveillance and foreign technical surveillance countermeasures believed to be employed or capable of employment against US installations or personnel.

c. With respect to audio countermeasures:

(1) To recommend to USIB departments and agencies and others as appropriate, and to coordinate the execution of, procedures for implementation of policies in the technical surveillance countermeasures field.

(2) To develop and recommend to the DCI standard security practices for use by US Government agencies and departments for defense against technical surveillance penetration, including standards for the security indoctrination of US personnel and coordinated training for technical inspectors.

(3) To ensure prompt notification of the chairman by USIB departments and agencies of the discovery or suspected presence of clandestine technical surveillance devices in US installations, including information on the possibility of exploitation.

d. With respect to countermeasures research and development:

(1) To foster an aggressive and imaginative program of research and development leading to improved technical surveillance countermeasures equipment and techniques.

(2) To coordinate research and development programs in the technical countermeasures field, particularly to ensure an effective exchange of information and to avoid unwarranted duplication.

4. Community responsibilities

a. Upon request of the committee chairman, USIB departments and agencies shall furnish to the committee within established security safeguards particular information, materials, and ad hoc temporary personnel support needed by the committee and pertinent to its functions.

b. Each USIB member is responsible for initiating the investigation of any unauthorized disclosure of intelligence, intelligence information or intelligence sources and methods. When the report of such an investigation involves or affects USIB interests or another USIB member, it shall be forwarded to the Security Committee for review and reporting in accordance with paragraph 3 a (8) above.

5. Composition and organization

a. The committee will consist of a full-time chairman designated by the DCI, representatives of the chiefs of departments and agencies who are members of the USIB, and representatives of the Departments of the Army, Navy and Air Force. The chairman may invite a representative of the chief of any other department or agency having functions related to matters being considered by the committee to sit with the committee whenever matters within the purview of that department or agency are to be discussed.

b. The committee will be supported by subcommittees as approved by the DCI and ad hoc working groups as approved by the chairman. The chairmen of subcommittees will be designated by the committee chairman with the concurrence of the DCI. Membership on the subcommittees and ad hoc working groups need not be limited to member agencies of

the committee, but may be extended by the chairman to representation of other departments and agencies having related functional responsibilities or support capabilities.

c. The committee will have a full-time support staff to be provided by USIB departments and agencies as arranged and approved by the DCI

6. Rules of procedure

a. The committee shall meet upon the call of the chairman or at the request of any of its members. Items may be placed on the agenda by the DCI or by the chairman or any member of the committee.

b. Decisions or recommendations will be formulated by the chairman with consideration given to the views of the members. At the request of a dissenting member, the chairman will refer the decision or recommendation along with dissenting opinion or opinions to the DCI.

c. The committee shall exercise primary responsibilities with respect to the mission and functions assigned to it, and shall coordinate with other committees established by DCIDs in areas of joint or overlapping concern. In submitting its recommendations to the DCI, the committee will specify any unresolved questions as between this committee and related committees which, under other DCIDs, continue to have responsibilities for security matters within their respective jurisdictions.

d. The committee shall submit an annual report to the DCI upon his call.

W. E. Colby
Director of Central Intelligence